CISCO AMP FOR ENDPOINTS CASE STUDY

S&P 500 Telecommunications Services Company

Introduction

This case study of an S&P 500 telecommunications services company is based on a January 2020 survey of Cisco AMP for Endpoints customers by TechValidate, a 3rd-party research service. The profiled company asked to have their name blinded to protect their confidentiality.

> “AMP for Endpoints has greatly expedited our incident response efforts by providing forensic data we didn’t have access to with other products.”

Challenges

The business challenges that led the profiled company to evaluate and ultimately select Cisco AMP for Endpoints:

- Invested in Cisco AMP for Endpoints because they:
  - Needed to protect against advanced threats
  - Needed tools to enhance their threat hunting capabilities
  - Watned better forensics and visibility into what was happening on the endpoint on an alert
- Considered the following vendors before selecting Cisco AMP for Endpoints:
  - Microsoft
  - Symantec
  - TrendMicro

Use Case

The key features and functionalities of Cisco AMP for Endpoints that the surveyed company uses:

- Other Cisco Security products used in addition to Cisco AMP for Endpoints:
  - Umbrella
  - Email Security
  - NGFW (Next-Generation Firewall)
  - DUO (Multi-Factor Authentication/MFA)
  - AnyConnect
- Rates Cisco AMP for Endpoints on the following features:
  - Antivirus feature: blocking known malware: extremely satisfied
  - Exploit prevention feature: protecting against file-less malware: extremely satisfied
  - Threat detection and response feature: continuous file monitoring (file and device trajectory): extremely satisfied
  - Threat intelligence: ability to understand unknown threats to their environment: extremely satisfied
  - Multi-platform/OS support: extremely satisfied

Results

The surveyed company achieved the following results with Cisco AMP for Endpoints:

- Most prominent benefits realized from their investment in Cisco AMP for Endpoints:
  - Realized better overall protection/prevention against file-less malware, ransomware, and other advanced threats
  - Experienced faster and more accurate threat detection and remediation
  - Experienced faster, more effective incident response
  - Enhanced threat hunting capabilities
- Experienced the following after implementing Cisco AMP for Endpoints:
  - Improved threat detection and remediation speed and quality: 50% to 74%
  - Improved incident response speed and effectiveness: 50% to 74%
- Cisco AMP for Endpoints helped their security team to better protect their environment from:
  - Zero-day threats
  - Ransomware
  - Cryptomining
- Their confidence in protecting their endpoints against malware and other threats has improved now that they have Cisco AMP for Endpoints as part of their security strategy.
- Reduced their time to detection of threats by more than a day after implementing Cisco AMP for Endpoints.

Company Profile

The company featured in this case study asked to have its name publicly blinded because publicly endorsing vendors is against their policies.

TechValidate stands behind the authenticity of this data.

Company Size:
S&P 500

Industry:
Telecommunications Services

About Cisco AMP for Endpoints

Get global threat intelligence, advanced sandboxing, and real-time malware blocking to prevent breaches with Cisco Advanced Malware Protection (AMP). But because you can’t rely on prevention alone, AMP also continuously analyzes file activity across your extended network, so you can quickly detect, contain, and remove advanced malware.

Learn More:

Cisco

Cisco AMP for Endpoints

Source: TechValidate survey of a S&P 500 Telecommunications Services Company

Research by TechValidate by SurveyMonkey

✓ Validated Published: Mar. 10, 2020 TVID: 554-834-6BB